This application is a continuation in part of Application number 09/554,518 entitled SYSTEM AND METHOD OF AUTHENTICATING A KEY AND TRANSMITTING SECURE DATA and filed May 11, 2000.

NOTE: 1. With respect to the detailed explanation, we have tried to clarify.

NOTE: 2. With respect to Thomlinson, we believe there has been a misunderstanding on the part of the examiner and have made extensive notes. It is to be noted that there must be some overlap because of the nature of computer systems and computer software, but taken in the context of this application, the invention is both novel and innovative and cannot be inferred from other prior art.

In the Detailed Description of the Invention:

Replace the replace the Detailed Description as follows:

DETAILED DESCRIPTION OF THE INVENTION

The following is a detailed description of illustrative embodiments of the present invention. As these embodiments of the present invention are described with reference to the aforementioned illustrations, various modifications or adaptations of the methods and or specific structures described may become apparent to those skilled in the art. All such modifications, adaptations, or variations that rely upon the teachings of the present invention, and through which these teachings have advanced the art, are considered to be within the spirit and scope of the present invention. Hence, these descriptions and

drawings should not be considered in a limiting sense, as it is understood that the present invention is in no way limited to only the embodiments illustrated.

Referring now to FIG. 1, a schematic diagram illustrates a web server 100 and a client computer 102 connected to the Internet 110. For security purposes, the client computer 102 has a RF reader (radio frequency reader) 104 for reading a RF smart card 106 having a user's private key. The RF smart card could also be a contact smart card or an alternate personal storage device, like a USB memory drive or a memory card. All of these devices will be referred to as the RF smart card, hereafter. The private key on the RF smart card 106 can be very long (i.e. 1000 bytes) and could include any type of biometric data, such as a digitized fingerprint of the user. The private key here is to be distinguished from other types of private keys and is in fact more correctly described as personal user data. The private key could be very long and any data that is encrypted using this private key would be virtually impossible to decrypt by a hacker, since this private key can be much longer than a typical private key (64 bytes) used in a private/public key system. The client 102 also has a fingerprint scanner 108 for helping to authenticate the private key of the user. Biometric readings employed by this invention are not limited to fingerprints. Other types of biometric readings can also be used, such as the reading from the eye and analysis of the face. A special biometric composed of a random string can also be used and assigned

to the user. This personal random string will be referred to as a "Pseudo Biometric" henceforth.

FIG. 2 is a block diagram of the client computer 102 shown in FIG. 1. Computer 102 includes a CPU 202, a RAM 204, a non-volatile memory 206, an input device 208, a display 210, an Internet interface 212 for providing access to the Internet, a RF reader interface 214, and a fingerprint scanner interface 216. Again it is to be noted that the RF reader is symbolic of a reader for a personal storage device and the fingerprint scanner is symbolic of any biometric scanning device.

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module 206 located within the client computer 102 of FIG. 2. The non-volatile memory 206 includes an encrypt/decrypt engine 302 for encrypting and decrypting data.

The encrypt/decrypt engine 302 is programmed to encrypt and decrypt data using a password or a key. Excellent results can be obtained when using the blowfish algorithm for encryption and decryption. Other types of symmetric key encryption/decryption algorithms can also be employed within the encrypt/decrypt engine 302.

FIG. 4 is a flowchart of a method illustrating the authentication of a key at a client computer in accordance with the invention. The authentication process begins at step 400. The authentication process includes three security levels, however, not every level of security is required to authenticate the key of the user. Depending on

the type of application, only one or two of the security levels may be employed.

Security level I 402 begins at step 404 where the user scans his user's RF key card 106 with the RF reader 104. Security level II 406 then begins at step 408 where the user enters his password at the client computer 102. At step 410 the data scanned from the user's RF key card is decrypted with the encrypt/decrypt engine 302 using the user's password. It is to be noted that encrypt/decrypt here refers to the extraction of the data from the storage device into a non encrypted state.

At step 414, security level III 412 begins and a digitized fingerprint scan is taken from the user. At step 416 the digitized fingerprint scan is compared with the data decrypted from the RF key card. At step 418 it is determined if there is a probabilistic match between the digitized fingerprint scan and the data decrypted from the RF key card. If it is determined that there is not a match, then at step 420 the authentication of the user's key fails and is rejected. If at step 418 it is determined that there is a match, then at step 422 the user's key is authenticated. The decrypted data from the RF key card can then be used as an authenticated encryption key for sending data to a server over and unsecure network, such as the Internet. Here, it is to be noted that all of the formation of the users encryption key applies locally and that none of the data is sent to the server. This invention applies to a personal device that can be utilized to form a personal

user key that is subsequently used for other security purposes.